REMARKS

After entry of the foregoing amendment, claims 8-13 remain pending in the application.

The cancellation of claims 1-7 is without prejudice; applicant may continue their prosecution in a related application.

The allowance of claims 8-13 is noted with appreciation. Only allowed claims now remain in the application, so the application is believed to be in condition for allowance.

In their last Amendment, applicant noted claims pending in – and prosecution in – related application 09/479,304. A copy of the latest Action in that case – and applicant's response – are submitted herewith as Appendices A and B to these Remarks.

Additionally, the Examiner's attention is drawn to copending application 11/670,841, which is understood to be on the present Examiner's docket. An Action was issued in that case on September 14, 2007 (copy attached as Appendix C), concerning the following pending claims:

> 1. A method of operating a wireless telephone device, characterized by decoding plural-bit data steganographically encoded in digital information processed by said wireless telephone device, and controlling an aspect of the device's operation based on said decoded data.
>
> 2. The method of claim 1, characterized by decoding said plural-bit data in accordance with pseudo-random key information.
>
> 3. The method of claim 1, further characterized by filtering said digital information before decoding the plural-bit data steganographically encoded therein.
>
> 4. The method of claim 1, further characterized by performing a mean-removal operation on said digital information before decoding the plural-bit data steganographically encoded therein.
>
> 5. The method of claim 1 in which said decoding includes performing a matched filtering operation.

6. The method of claim 1 in which said decoding includes performing a correlation operation.

7. The method of claim 1 in which said decoding includes determining a correct alignment of the digital information before decoding the plural-bit data steganographically encoded therein.

8. The method of claim 1 that includes receiving said digital information from a data channel on which it is sent in the form of packets.

9. The method of claim 1 that includes decoding plural-bit data steganographically encoded in digital information wirelessly received by said device.

10. The method of claim 1 that includes decoding plural-bit data steganographically encoded in digital audio information processed by said device.

11. A method for checking whether data transmitted in a telephone call has been altered, comprising:

receiving a telephone call;

extracting audio data from the telephone call; and

checking whether the telephone call has been altered by extracting auxiliary data embedded in the audio data and checking whether the extracted auxiliary data satisfies a predetermined relationship with data associated with the telephone call.

12. A method comprising:

receiving a 911 emergency call; and

recording the call;

wherein prior to said recording, the audio of said call is steganographically encoded with plural-bit hidden data so as to facilitate later authentication.

21. A wireless telephone device characterized by a steganographic decoder operative to recover steganographically encoded data from digital information processed by said device, and further including a processor operative to control an aspect of the wireless telephone device's operation based on the recovered data.

22. The device of claim 21 that further includes a microphone, a modulator, an antenna, and an RF amplifier.

23. The device of claim 21, in which said steganographic decoder is operative to recover steganographically encoded data from digital audio processed by said device.

Favorable consideration and passage to issuance are solicited.

Respectfully submitted,

DIGIMARC CORPORATION

Date: November 9, 2007

Customer Number 23735

Phone: 503-469-4800
FAX 503-469-4777

By_____
William Y. Conwell
Registration No. 31,943

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/479,304	01/06/2000	GEOFFREY B. RHOADS	60085	2884

23735 7590 08/08/2007

DIGIMARC CORPORATION
9405 SW GEMINI DRIVE
BEAVERTON, OR 97008

EXAMINER	
PICH, PONNOREAY	
ART UNIT	**PAPER NUMBER**
2135	
MAIL DATE	**DELIVERY MODE**
08/08/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Docketed: 10-8-07
11-8-07
Book: Init:

AUG 10 2007

EXHIBIT A

Application No.	Applicant(s)	
09/479,304	RHOADS, GEOFFREY B.	
Examiner	**Art Unit**	
Ponnoreay Pich	2135	

Office Action Summary

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 May 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *52-72* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *52-72* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *11/06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

EXHIBIT A

DETAILED ACTION

Claims 1-52 are cancelled. Claims 52-72 were newly added and are pending.

Information Disclosure Statement

The documents listed in the IDS submitted on 11/8/2006 were considered. The examiner has crossed out some documents because they were already cited in either a previously submitted IDS or in an 892 form submitted by the examiner. As such, it is redundant to list them once more.

Response to Arguments

Applicant's arguments that the prior art of record (Reeds and Hopper) do not teach the limitations not claimed were considered. The arguments were not persuasive. Please see further clarification below in the rejection of the claims. As per applicant's argument which was directed towards the motivation to combine, please note that the motivation given below for combining the teachings of Reeds and Hopper came from the prior art themselves. Note that the rationale to modify a prior art invention may be expressly or impliedly contained in the prior art or it may be reasoned from knowledge generally available to one of ordinary skill in the art, established scientific principles, or legal precedent established by prior case law. In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); In re Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, because the motivation came from the prior art, the motivation is valid.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 59 and 65 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

1. Claim 59 recites "the plural-bit auxiliary code" which lacks antecedent basis. The examiner will assume applicant meant "a plural-bit auxiliary code".
2. Claim 65 recites "the hidden code" in the last line, which the examiner believes should be "the hidden plural-bit auxiliary code".

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 52-54, 58-59, 72, 55-57, and 60-65 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reeds, III et al (US 5,204,902) in view of Hopper (US 3,406,344).

Claim 52:

Reeds discloses a cell phone including a radio receiver circuitry (Fig 11, item 220), a memory (Fig 11, item 240), a data capture system and a radiant-energy digital data transmission system (Fig 11; col 4, lines 5-9; and col 11, lines 16-27 and 65-66). Note that all cell phones have a data capture system, i.e. microphone for a user to speak into.

Reeds further discloses that the cell phone is characterized in that the cell phone further includes an encoder that alters data captured by the data capture system in accordance with an encoding signal prior to transmission by the data transmission system (col 7, lines 21-34; col 9, lines 28-45; and col 11, lines 21-27). Note that the cited sections discusses that a RAND sequence is broadcasted from a base station to the cell phone. The cell phone uses the RAND sequence as an input into a Jumble process to generate an encoding signal, i.e. bits of group A, which is used to encode/encrypt the user's speech received by the cell phone before transmission.

Reeds further discloses wherein the encoder is adapted to generate an encoding signal that depends, at least in part, on information received by the radio receiver circuitry and stored in the memory (col 7, lines 21-34; col 9, lines 28-45; col 11, lines 21-27 and lines 65-66). The RAND signal was received by the cell phone and stored in block 240. The encoding signal, i.e. bits of group A, is generated at least in part from the RAND signal received by the cell phone. The RAND signal is interpreted to be the claimed information received by the radio receiver circuitry and stored in the memory.

Reeds does not explicitly disclose that the encoder is a steganographic encoder and the encoding is steganographic encoding. However, Hopper discloses use of a

steganographic encoder to perform steganographic encoding in a telephone system (col 1, lines 11-21 and 37-62). Note modulating the auxiliary data signal so that it is found in the speech signal's sideband such that the auxiliary signal is transmitted at the same time as the speech signal without interfering with the speech signal in any perceptible manner is steganographic encoding of the speech signal with the auxiliary signal.

Reeds and Hooper's disclosures are both from the telecommunication field. At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to modify Reeds's invention using Hopper's teachings such that Reeds's cell phone also used steganography to redundantly encoded the user's voice signal by hiding an auxiliary identification signal in the voice signal before transmission. One skilled would have been motivated to do so because Hopper discloses that it is desirable for data service to coexist with speech service for various reasons, i.e. to identify the source of a call (col 1, lines 37-63).

Note that the RAND signal disclosed by Reeds is used for authentication purposes, and as such the RAND signal would have been an obvious choice to create an auxiliary authentication signal from with which to use in steganographic encoding of the voice signal for line/caller identification purposes as per Hopper's teachings. Reeds discloses that to enhance security the cell phone is re-authenticated periodically (col 9, lines 24-25 and 47-50). Using Hopper's teachings to achieve re-authentication is an obvious choice because Hopper discloses that redundantly encoding a signal into the voice data for identification purposes would reduce the error rate in reception (col 4, lines 65-71). Whenever the base station of Reeds's modified invention wanted to re-

authenticate the cell phone, all it has to do is check the authentication data that was steganographically encoded onto the voice data.

Note that the examiner has determined that one of ordinary skill in the art would be an engineer having significant experience in the telecommunication industry and is familiar with different ways of encoding transmitted signals, including using steganography to encode a signal.

Claim 53:

Reeds further discloses that the data capture system captures audio, i.e. speech, and includes a microphone (col 9, lines 28-31). Note that all cell phones includes microphones to capture speech from the user.

Claim 54:

As per claim 54, Hopper further discloses that the steganographic encoder is adapted to operate transparently to a user of the telephone (col 1, lines 37-41 and col 4, lines 44-58), wherein all of the data captured by the data capture system and transmitted by the telephone is steganographically encoded (col 4, lines 44-58 and 67-73).

One skilled should appreciate that when two users speak to each other via a telephone system, any delay due to encoding of the signal for transmission is not noticed by the users, i.e. the encoding is transparent to the user. In the cited portions of Hopper, the auxiliary data signal is transmitted at the same time as the voice signal without any action being taken by the user except for the user to speak as he/she would normally do when using a telephone. Hopper's invention continuously monitors for

speech energy bursts via detector 13 and only when a burst is detected is the auxiliary data signal supplied for modulation with the speech signal. Further, Hopper discusses that it is preferred that the auxiliary code word is repetitively transmitted in the speech signal. This teaching would lead one of ordinary skill to steganographically encode all of the data captured by the data capture system since doing so would provide the maximum redundancy possible. The telephone being a cell phone is obvious over the additional teaching of Reeds.

Claim 58:

Hopper further discloses wherein the steganographic encoder is adapted to combine an overlay signal with the data captured by the data capture system (col 4, lines 44-58 and 67-73 and col 5, lines 3-30).

Note that the cited portions disclose a code word is redundantly transmitted as a sideband of the speech signal. The examiner is considering the signal created by repeating the code word for transmission as the claimed overlay signal. The speech signal is considered the data captured by the data capture system. Since the auxiliary data signal is transmitted simultaneously with the voice signal in the sideband of the voice signal, the overlay/auxiliary data signal is considered combined with voice signal.

Claim 59:

Hopper further discloses wherein the steganographic encoder is adapted to generate an overlay signal, i.e. the signal generated from repeating the code word, that is dependent on both a plural-bit auxiliary code and on the data captured by the data capture system (col 4, lines 44-58 and 67-73; col 5, lines 3-30; and col 6, lines 32-35).

Note that the data signal which is encoded onto to the voice signal is made up of code words. The examiner considers these disclosed code words as plural-bit auxiliary codes. In encoding the (auxiliary) data signal onto the voice signal, the cited section in column 5 discusses that the amplitude of the data signal is adjusted so that it does not cause a noticeable distortion in the speech signal. This adjustment to the data signal is done by measuring the magnitude of the speech burst. As such, the generation of the auxiliary data signal, i.e. the claimed overlay signal, is dependent on both the code words, i.e. plural bit auxiliary code, and on the speech bursts, i.e. the data captured by the data capture system.

Claim 72:

Hopper further discloses wherein the steganographic encoder is adapted to generate an encoding signal that also depends – in part – on dynamics of the data (col 4, lines 44-58 and 67-73; col 5, lines 3-30; and col 6, lines 32-35).

The examiner considers the auxiliary data signal which is encoded as a sideband signal of the speech signal to be the encoding signal. The cited portion of Hopper discusses how the amplitude of the auxiliary data signal is adapted so that it does not cause appreciable distortion in the speech signal. To do this, the magnitudes of individual speech bursts are measured. In other words, the amplitude of the generated encoding signal, i.e. the auxiliary data signal, is dependent at least in part on the dynamics of the data, i.e. speech signal, as measured by the magnitude of each speech burst.

Claim 55:

Reeds discloses:

1. Receiving input information, i.e. user's speech or voice data (col 4, lines 9-12 and col 9, lines 26-44).
2. Receiving data, i.e. RAND and/or RANDU sequence, wirelessly sent from a remote transmitter (col 7, lines 21-34; col 9, lines 28-45; col 11, lines 21-27 and lines 65-66).
3. Encoding the input information, the encoding depending, at least in part on the received data (col 7, lines 21-34; col 9, lines 28-45; col 11, lines 21-27 and lines 65-66). *Note that the RAND signal is used to create a group of bits, i.e. group A, which is used to encode/encrypt speech data. As such the encoding/encryption depends at least in part on the received RAND signal.*
4. Transmitting the encoded information by wireless in a digital format (col 4, lines 9-12; col 9, line 28-44; and col 11, lines 16-35).

Reeds does not explicitly disclose the encoding is steganographically encoding to hide a plural-bit auxiliary code and that the data transmitted is steganographically-encoded information. However, Hopper discloses steganographically encoding a plural-bit auxiliary code, i.e. code words, in received input information, i.e. voice data, and that the information transmitted from the telephone is steganographically-encode information (col 1, lines 11-21 and 37-62).

At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to modify Reeds's invention according to the limitations recited in

claim 55 in light of Hopper's teachings. One skilled would have been motivated to incorporate Hopper's teachings within Reeds's invention for the same reasons discussed in claim 52.

Claim 56:

Reeds further discloses:

1. Receiving the input information in a non-digital form (col 9, lines 28-44 and col 11, lines 21-27). *One skilled should appreciate that human speech is analog in nature. As such when the cell phone's microphone is used to receive the speech into the cell phone, the speech is received in analog format. Further evidence of this is that the information has to be converted into digital format. This means that the information was not in digital format when received.*
2. Expressing the received information in digital format (col 9, lines 28-44 and col 11, lines 21-27).
3. Encoding the digital form of the input information (col 9, lines 28-44).

Claim 57:

Reeds further discloses wherein the input information is audio information, i.e. speech (col 9, lines 28-44).

Claim 60:

Hopper further discloses wherein the steganographic encoding includes combining an overlay signal with the input information (col 4, lines 44-58 and 67-73 and col 5, lines 3-30).

Note that the cited portions disclose a code word is redundantly transmitted as a sideband of the speech signal. The examiner is considering the signal created by repeating the code word for transmission as the claimed overlay signal. The speech signal is considered the data captured by the data capture system. Since the auxiliary data signal is transmitted simultaneously with the voice signal in the sideband of the voice signal, the overlay/auxiliary data signal is considered combined with voice signal, i.e. input information.

Claim 61:

Hopper further discloses wherein the steganographic encoding includes combining an overlay signal with the input information (col 4, lines 44-58 and 67-73; col 5, lines 3-30; and col 6, lines 32-35).

Note that the cited portions disclose a code word is redundantly transmitted as a sideband of the speech signal. The examiner is considering the signal created by repeating the code word for transmission as the claimed overlay signal. The speech signal is considered the data captured by the data capture system. Since the auxiliary data signal is transmitted simultaneously with the voice signal in the sideband of the voice signal, the overlay/auxiliary data signal is considered combined with voice signal, i.e. input information.

Claim 62:

The limitations recited in claim 62 can all also be found in claims 52, 55, and 72 and as such, claim 62 is rejected over Reeds and Hopper for similar reasons discussed in claims 52, 55, and 72.

Claim 63:

Hopper further discloses the steganographic encoder is adapted to control an amplitude of the encoding signal, i.e. the auxiliary data signal, in part, in accordance with dynamics of the data, i.e. the speech signals (col 5, lines 3-30).

The examiner considers the auxiliary data signal which is encoded as a sideband signal of the speech signal to be the encoding signal. The cited portion of Hopper discusses how the amplitude of the auxiliary data signal is adapted/controlled so that it does not cause appreciable distortion in the speech signal. To do this, the magnitudes of individual speech bursts are measured. In other words, the amplitude of the generated encoding signal, i.e. the auxiliary data signal, is dependent at least in part on the dynamics of the data, i.e. speech signal, as measured by the magnitude of each speech burst.

Claim 64:

The limitations further recited in claim 64 are substantially similar to limitations found recited in claim 52 and as such claim 64 is rejected for similar reasons discussed in claim 52.

Claim 65:

Most of the limitations recited in claim 65 are also found in claims 52 and 55 and these limitations are rejected for similar reasons discussed in claims 52 and 55. Claim 65 additionally recites "the steganographic encoder being adapted to introduce a pseudo-random signal to the data in which the hidden plural-bit auxiliary code is encoded". This limitation reads on encrypting the steganographically encoded data

signal using a randomly generated key. Official notice is taken that encrypting signals with a random key was well known in the art. At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to further modify Reeds's invention such that the steganographic encoder was encrypted by introducing a pseudo-random signal to the data after the data signal was encoded by hiding the plural-bit auxiliary code within the data signal. One skilled would have been motivated to do so because it would ensure private communication on the cell phone. One skilled would have been motivated to use a pseudo-random signal as the encryption key because they offer a high level of security. Note that in just relying on steganography alone, an eavesdropper can still listen in on a cell phone call electronically. Note that Reeds was interested in encryption of the speech data (col 9, lines 24-25).

Claims 66-69 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reeds, III et al (US 5,204,902) in view of Hopper (US 3,406,344) and further in view of Lee et al (US 5,687,191) and as evidenced by Jones (3,586,781).

Claim 66:

Most of the limitations recited in claim 66 are also found in claims 52 and 55 and these limitations are rejected for similar reasons discussed in claims 52 and 55. Claim 66 additionally recites "the host data comprising sample values, and the steganographic encoder being adapted to increase certain of the sample values and decrease others."

Hopper discloses the host data, i.e. voice data, comprising sample values, i.e. speech bursts (col 4, lines 44-49 and col 5, lines 3-30).

Reeds and Hopper do not explicitly disclose the steganographic encoder being adapted to increase certain of the sample values and decrease others. However, the limitation is disclosed by Lee (col 7, lines 34-44). The cited portion of Lee discusses that each samples' amplitude are analyzed and normalized. Normalization of the amplitude implies that the amplitude of samples that were above the mean value were decreased, while the amplitude of samples that were below the mean value were increased.

At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to further modify Reeds' invention according to the limitations recited in claim 66 in light of Lee's teachings. One skilled would have been motivated to do so because as evidenced by Jones, speech signals typically vary over a dynamic range, some being very loud, i.e. having high amplitude, while others are very soft, i.e. having low amplitude, and modulating the amplitude of the speech samples so that they were more uniform, i.e. normalized, would improve the quality of transmissions (Jones: col 1, lines 28-36 and 65-69).

Claim 67:

Reeds, Hoper, and Lee do not explicitly disclose wherein the steganographic encoder is adapted to increase certain of the sample values between 7.5% and 100%. However, as discussed in claim 66, as per Lee's teachings, it would improve transmission if the amplitude of the host data, i.e. voice samples, were normalized. This

would mean that the amplitude of some of the samples would be increase, while some were decreased. It would not be unexpected that in normalizing some of the samples having low amplitude that the amplitudes may increase anywhere from 7.5% and 100%. It would not be unreasonable to assume that one of ordinary skill would try different percentages of increasing the amplitude of the lower amplitude samples and in routine experimentation find that some of the samples should be increased anywhere from 7.5% to 100% to achieve better quality of transmission.

Claim 68:

The limitations further recited in claim 68 are similar to what is recited in claim 72 and are rejected for similar reasons. Note that the encoding referred to in claim 72 is steganographic encoding to hide the plural-bit auxiliary code as recited in claim 68.

Claim 69:

Claim 69 recites limitations similar to those found in claims 55 and 66 and as such claim 69 is rejected over Reeds, Hooper, Lee, and as evidenced by Jones for the reasons discussed in claims 55 and 66.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Thurs.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Ponnoreay Pich
Examiner
Art Unit 2135

PP

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

EXHIBIT A

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Art Unit: 2135

Geoffrey B. Rhoads Confirmation No.: 2884

Application No.: 09/479,304

Filed: January 6, 2000

For: WIRELESS METHODS AND DEVICES EMPLOYING STEGANOGRAPHY

VIA ELECTRONIC FILING

Examiner: P. Pich

Date: October 11, 2007

AMENDMENT ACCOMPANYING RCE

COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

Sir,

Responsive to the Final Action mailed August 8, 2007, and prior to further examination, please amend the subject application as follows:

EXHIBIT B

In the Claims:

1-51. (Canceled)

52. (Currently Amended) A cell phone including radio receiver circuitry, a memory, a data capture system and a radiant-energy digital data transmission system, characterized in that the cell phone further includes a steganographic encoder that alters data captured by the data capture system in accordance with an encoding signal prior to transmission by the data transmission system, wherein the steganographic encoder is adapted to generate an encoding signal that depends, at least in part, on information received by the radio receiver circuitry and stored in the memory, **wherein data captured by the data capture system is digitally marked with the encoding signal prior to being transmitted by the data transmission system**.

53. (Previously Presented) The cell phone of claim 52 in which the data capture system captures audio and includes a microphone.

54. (Previously Presented) The cell phone of claim 52 in which the steganographic encoder is adapted to operate transparently to a user of the cell phone, wherein all of the data captured by the data capture system and transmitted by the cell phone is steganographically encoded.

55. (Currently Amended) A method of operating a cell phone, comprising:

receiving input information;

receiving data wirelessly sent from a remote transmitter;

steganographically encoding the input information to hide a plural-bit auxiliary code therein, the encoding depending, at least in part, on the received data; and

transmitting the steganographically-encoded information by wireless in a digital format;

wherein the input information is digitally marked with the plural-bit auxiliary code prior to being transmitted.

56. (Previously Presented) The method of claim 55 which includes:
receiving the input information in non-digital form;
expressing the received information in digital form; and
encoding the digital form of the input information.

57. (Previously Presented) The method of claim 56 in which the input information is audio information.

58. (Currently Amended) The cell phone of claim 52 wherein the steganographic encoder is adapted to **additively** combine ~~an overlay~~ **a digital overlay** signal with the data captured by the data capture system.

59. (Currently Amended) The cell phone of claim 58 wherein the steganographic encoder is adapted to generate an overlay signal that is dependent both on ~~[the]~~ **a** plural-bit auxiliary code and on the data captured by the data capture system.

60. (Currently Amended) The method of claim 55 wherein the steganographic encoding includes **additively** combining ~~an overlay~~ **a digital overlay** signal with the input information.

61. (Previously Presented) The method of claim 60 wherein the overlay signal is dependent both on the plural-bit auxiliary code and on the input information.

62. (Currently Amended) A cell phone including a data capture system and a radiant-energy transmission system, characterized in that the cell phone further includes a steganographic encoder that modifies data captured by the data capture system in accordance with an encoding signal, to hide a plural-bit auxiliary code within the data prior to transmission by the data transmission system, the steganographic encoder being adapted to generate an encoding signal that depends - in part - on dynamics of the data, **wherein data captured by the data capture system is digitally marked with the encoding signal prior to being transmitted by the transmission system**.

63. (Previously Presented) The cell phone of claim 62 in which the steganographic encoder is adapted to control an amplitude of the encoding signal, in part, in accordance with dynamics of the data.

64. (Previously Presented) The cell phone of claim 62 further comprising wireless receiver circuitry that provides information to a memory, wherein the steganographic encoder is adapted to generate an encoding signal that depends, in part, on the information in the memory.

65. (Currently Amended) A cell phone including a data capture system and a radiant-energy transmission system, characterized in that the cell phone further includes a steganographic encoder that hides a plural-bit auxiliary code within data captured by the data capture system prior to transmission by the data transmission system, the steganographic encoder being adapted to introduce a pseudo-random signal to the data in which the hidden **plural-bit auxiliary** code is encoded, **wherein data captured by the data capture system is digitally marked with the plural-bit auxiliary code prior to being transmitted by the transmission system**.

66. (Currently Amended) A cell phone including a data capture system and a radiant-energy transmission system, characterized in that the cell phone further includes a steganographic encoder that hides a plural-bit auxiliary code within host data captured by the data capture system prior to transmission by the data transmission system, the host data comprising sample values, and the steganographic encoder being adapted to increase certain of the sample values and decrease others, **wherein data captured by the data capture system is digitally marked with the plural-bit auxiliary code prior to being transmitted by the transmission system**.

67. (Previously Presented) The cell phone of claim 66 wherein the steganographic encoder is adapted to increase certain of the sample values between 7.5% and 100%.

68. (Previously Presented) The cell phone of claim 66 wherein the steganographic encoder is adapted to respond to dynamics of the host data in hiding of the plural-bit auxiliary code within the host data.

69. (Currently Amended) A method of operating a cell phone, comprising:

receiving sampled input information;

steganographically encoding the input information to hide a plural-bit auxiliary code therein; and

transmitting the steganographically-encoded information from the cell phone in a digital format;

wherein the steganographically encoding comprises – in a pseudo-random fashion - increasing the values of certain samples and decreasing the values of other samples, the increasing and decreasing depending, in part, on dynamics of the sampled input information, **and wherein the input information is digitally marked with the plural-bit auxiliary code prior to being transmitted**.

70. (Previously Presented) The method of claim 55 that further includes wirelessly communicating an identifier from the cell phone, wherein said plural-bit auxiliary code is at least partially redundant with said identifier, so that at least part of said identifier is sent from the cell phone in two different manners.

71. (Previously Presented) The method of claim 55 wherein said plural-bit auxiliary code comprises an identifier uniquely identifying the cell phone, rather than identifying the input information or a user of cell phone.

72. (Previously Presented) The method of claim 52 wherein the steganographic encoder is adapted to generate an encoding signal that also depends – in part – on dynamics of the data.

73. (New) The cell phone of claim 62 in which the data comprises a series of samples, and the steganographic encoder is adapted to generate an encoding signal that depends on the dynamics of several samples.

74. (New) The cell phone of claim 62 in which the steganographic encoder is adapted to generate an encoding signal that is responsive to a first-, second- or higher-order derivative of the data.

75. (New) A method of steganography usage in a wireless phone device, comprising:

receiving data wirelessly sent from a remote transmitter;

generating an encoding signal that depends on said received data wirelessly sent from the remote location;

altering digital data in accordance with said encoding signal to yield steganographically encoded data; and

wirelessly transmitting the steganographically-encoded data from the wireless phone device to a remote location.

76. (New) A method of steganography usage in a wireless phone device, comprising:

by reference to input digital data and to plural-bit auxiliary data, generating an encoding signal that represents said plural-bit auxiliary data and that depends, in part, on said input digital data;

altering said input digital data in accordance with said encoding signal to yield steganographically encoded data; and

wirelessly transmitting the steganographically-encoded data to a remote location.

77. (New) A method of steganography usage in a wireless phone device, comprising:

wirelessly communicating an identifier from said wireless phone device to a remote location; and

separately, conveying at least a portion of said identifier from said wireless phone device to said remote location through use of steganographic encoding of an information signal transmitted by said wireless phone device;

wherein said identifier is sent from said wireless phone device in two different manners.

78. (New) A method of steganography usage in a wireless phone device, comprising:

in a first transmission of information from said wireless phone device, steganographically encoding the information with a first encoding signal;

in a subsequent transmission of information from said wireless phone device, steganographically encoding the information with a second encoding signal different than the first;

wherein said first and second encoding signals differ by reason of at least one of the following:

different first and second data wirelessly received by said wireless phone device from a remote location, on which said encoding signals depend; or

the first encoding signal encodes a first identifier, and the second encoding signal also encodes said first identifier, but represents said first identifier with a different encoding signal than the first encoding signal.

79. (New) A method of steganography usage in a wireless phone device, comprising:

processing an information signal to steganographically encode the information signal with auxiliary data including an identifier;

modulating a carrier signal with said steganographically encoded information signal; and

transmitting said modulated carrier signal;

wherein said identifier comprises data uniquely identifying the wireless device, rather than identifying the information signal or a user of said wireless phone device.

80. (New) A wireless phone device including a data capture system, a radiant-energy digital data transmission system, and radio receiver circuitry, characterized in that the wireless phone device includes processing circuitry and memory, the memory containing programming causing the processing circuitry to perform the following acts:

store data obtained by use of said radio receiver circuitry;

generate an encoding signal that depends, at least in part, on said stored data; and

alter a representation of data captured by the data capture system in accordance with said encoding signal to yield a steganographically encoded signal;

wherein said digital data transmission system includes an input to which said steganographically encoded signal is provided.

REMARKS

After entry of the foregoing amendment, claims 52-80 are pending in the application. Claims 73-80 are newly added.

New claims 75-80 are renumbered counterparts of independent claims submitted in the present case with an Amendment dated November 8, 2006. Those claims were withdrawn from consideration as directed to a non-elected invention (January, 2007 Action). However, since that Amendment was deemed "non-responsive" to the previous Action, it is not clear if the claims were ever formally entered in the present application.

So as to provide an unambiguous record, the claims are re-presented with this RCE application. They may again be found to be restrictable, for the same reasons detailed in the January, 2007 Action.

Applicant has amended claims 59 and 65, per the Examiner's suggestion, to overcome the § 112 rejections.

Claims 52-65 and 72 stand rejected as unpatentable over Reeds (5,203,902) in view of Hopper (3,406,344).

Reeds concerns an arrangement by which "secret data" can be shared between a cell phone handset and a local cell base station, for authentication and encryption purposes.

In his Background discussion Reeds notes that various authentication arrangements are known, e.g., using private keys and public/private key pairs, and that same have been used to validate a cell phone transaction at the time a call is made. However, Reeds explains that such arrangements are unsatisfactory because the back-and-forth protocols associated with key exchange and verification are too slow for consumer acceptance. Waiting seconds to get a dial tone is generally intolerable (*c.f.*, col. 2, lines 8-15).

Reeds' invention addresses this authentication delay problem by conducting authentication infrequently, i.e., only when a handset first enters a local base station's coverage area (*c.f.*, col. 3, lines 31-36). Much of the back-and-forth of prior art

techniques is thus obviated, because both the handset and the local base station already share a "secret" that enables them to communicate securely.

At the outset (e.g., at the time the customer's account is established), the handset is programmed with a phone number (MIN1), an area code (MIN2), and its own secret (A-key). Additionally, the handset was hardwired with an electronic serial number (ESN).

When the handset is first initialized, a processor within the handset's home cell service area (home CGSA) sends a random sequence (RANDSSD) to the handset, with a directive to create a SSD. The handset responds by concatenating its ESN, its A-key, and the RANDSSD sequence, and applying the Jumble digital signature process. (Col. 4, lines 47-55; col. 6, lines 3-11; Fig. 4).

The handset's home CGSA knows the handset's ESN and A-key, so it can perform the same calculation to independently compute the SSD (col. 6, lines 24-33).

The shared secret resulting from this process has two parts, SSD-A and SSD-B. The former is used to support handset authentication, while the second is used to encrypt the voice signal (col. 6, lines 12-16).

Reed also details a verification procedure to check that this common secret is, in fact, shared (col. 6, lines 34-60).

When the initialized handset thereafter enters a new cell coverage area, a registration process occurs – typically only once.

During this handset registration process, the handset receives a RAND sequence broadcasted by the local base station, and replies by sending the phone's phone number (MIN1), area code (MIN2), and serial number (ESN) in plaintext, as well as a hashed authentication string. This hashed authentication string is formed by concatenating RAND + ESN + MIN1 + SSD-A, and applying the Jumble procedure (col. 7, lines 21-34).

The local base station knows all of the foregoing information, except the handset's SSD-A (col. 7, lines 41-46). But from the handset's area code and phone number (MIN2 + MIN1), the local base station can lookup the handset's home CGSA, and it passes a request to the home CGSA for the SSD information – providing data known to the local base station, *i.e.,* the handset phone number, its ESN sequence, the

RAND sequence it issued, and the authentication string returned from the handset based on, *inter alia,* that RAND sequence (col. 7, lines 46-55).

From the handset number (MIN1), the home CGSA looks up the earlier-established shared secret (SSD) and perform the Jumble operation earlier performed by the handset, *i.e.*, Jumble{RAND+ESN+MIN+SSD.A} to independently compute the authentication string. It compares this with the authentication string received from the local base station and, if they match, the home CGSA forwards the shared secret data (SSD) to the local base station (col. 7, lines 56-68).

By the foregoing registration process, the local base station knows the SSD (and the ESN) of the handset in its service area, and can use this information immediately to validate calls from the handset as they are set-up. In particular, when the handset makes a call, it receives the RAND signal then being broadcast by the local base station, concatenates it with the handset ESN, the shared secret data SSD-A, and the called party's phone number (MIN3), and applies the Jumble procedure. The base station does a parallel operation, and compares the two resulting strings for a match. This operation, and the comparison, are completed quickly (no multi-part exchanges are required), and the base station allows the call to proceed (col. 8, line 61 – col. 9, line 8).

Reed also encrypts the digitized speech transmitted from the handset for further security. In particular, he encrypts the speech using a key produced by applying the Jumble process to {RAND + ESN + MIN1 + SSD-B}. Since the local base station has all this data, it can immediately decrypt the transmitted speech.

In encrypting the speech, it will be recognized that Reed's goal is to achieve security by *preventing access* to the speech by eavesdroppers. He has effectively put the speech intelligence under lock and key, so that only a party with the Jumble-computed key can gain access to it. This is a legitimate theory of security, but it is not the one to which the claimed combinations are directed.

Instead of *preventing access* to speech transmitted by a cell phone, applicant's invention is concerned with *marking* speech transmitted by a cell phone – simply providing a method by which it can be identified. This is a different theory of security.[1]

Consider, as an analogy, a physical article, such as a bicycle. One theory of security says that the bicycle should be kept locked-up, so that only the owner (with the key) can access it. That way it can't get stolen by third party.

A different theory of security says that the bicycle should be labeled with the owner's name and phone number. Others may access it. But because it is marked with the owner's identity, it is unlikely to be stolen by a third party.

Local police often lend metal engraving tools to citizenry for just this purpose – to mark items of value as a deterrent against theft. Attached, as Exhibit A, is a bulletin from the Oregon State University Department of Public Safety, and the Oregon State Police, noting that engravers are available for check-out from a variety of providers, for marking bicycles, stereos, computers, etc., "to help deter theft."

Another relevant example is the current debate about the distribution of electronic music and video files. Should they be distributed with restrictive Digital Rights Management (DRM) provisions - effectively locking them to particular devices on which the content can be played (e.g., only Microsoft's Windows Media Player, or only Apple's iPods)? Or is it preferable for the files to be distributed in a form in which they can be played on all player devices – with unauthorized distribution being deterred by subliminally marking the name of the original owner into the file data (so that content on pirate sharing networks can be traced back to a possible source of the leak)? Both theories have their advantages and disadvantages.

The latter arrangement has been successfully used to mark "screener" videos distributed to members of the Academy of Motion Pictures Arts and Sciences (the voters for the Oscar awards). In 2004, two men were prosecuted for distributing pirated copies of academy screeners. An FBI investigation revealed that actor and Academy voter

[1] Of course, encryption can be employed with the presently-claimed arrangements as a further layer of security; however, it does not form part of the claimed arrangements, *per se*.

Carmine Caridi shipped dozens of screener DVDs to a friend. The friend uploaded those movies to file sharing sites, but the files contained watermarks that investigators used to trace their origin back to Caridi. Caridi was expelled from the Academy. (See FBI Press Releases attached as Exhibits B and C.)

Applicant's claims are amended, above, to emphasize the "marking" purpose to which his arrangements are directed.

Turning to the claims, applicant requests reconsideration of the rejections.

As a preliminary matter, applicant does not agree with the premise from which the Office's rejection starts, i.e., that because "*Reeds and Hopper's disclosures are both from the telecommunication field*" that they are properly combinable. This assertion proves too much.

If all telecommunications inventions having antecedents in the telecommunications field were obvious, then essentially nothing in the field of telecommunications would be patentable. It is natural, and proper, that inventors draw from work in their own field.

A more accurate starting point, applicant suggests, is to start with the arguably closest reference, Reeds, and inquire what motivation might an artisan find to alter Reeds (e.g., what shortcoming or deficiency would an artisan recognize). *Then,* based on that motivation, what art would the artisan logically look to?

To start with Reeds and Hopper at the outset - as was done in the present case – unfairly abbreviates the process, and shortchanges the proper role of the hypothetical artisan in the analysis.

As a second ground of traverse, applicant submits that – even starting with Reeds and Hopper – the motivation to combine offered by the Action is illusory.

The Action contends that an artisan would modify Reeds to incorporate Hopper's teachings "because it is desirable for data service to coexist with speech service for various reasons, *i.e., to identify the source of a call."*

EXHIBIT B

Hopper is not needed for this. Reeds already identifies the source of the call. Reeds' call set-up involves transmission of data based on the handset's electronic serial number (ESN) to the local base station. The base station thus can identify the source of the call. (If it didn't know the ESN of the handset, the base station couldn't validate the call.)

Reeds also identifies the source of the call throughout its duration. As noted in the Action, Reeds encrypts the speech sent to the base station. The encrypted speech is based on the handset's ESN and phone number. Again, the base station's successful decryption of the speech confirms the identity of the source of the call to the base station.

Thus, "to identify the source of a call" is an illusory reason to turn to Hopper's teachings; Reeds already identifies the source of the call.

As a third ground of traverse, applicant respectfully submits that – even if the Action's illusory motivation were pursued - the combination of Reeds and Hopper would not lead to the arrangement claimed.

As noted, the Office proposes that an artisan would have been motivated to employ Hopper's teachings in Reeds "because Hopper discloses that it is desirable for data service to coexist with speech service for various reasons, i.e., to identify the source of a call (col. 1, lines 37-63)."

In the cited passage, Hopper teaches that it is desirable to encode a telephone transmission with the information identifying the caller "*in order to identify the source of annoying or threatening telephone calls.*"

However, an artisan seeking to employ such teaching in Reed would not yield the arrangement of claim 52. In particular, an artisan would not be led to an arrangement in which the "encoding signal" (with which the transmission is marked) "*depends, at least in part, on information received by the radio receiver circuitry and stored in the memory.*"

Hopper teaches that his telephone transmission be marked with an identifier of the caller. Such information is available in Reeds' cell system in the form of the caller's phone number (MIN2 + MIN1), or by the handset's electronic serial number (ESN). Such data is pre-existing in the handset. An artisan following Hopper's teaching – in

Reeds' cell phone – would mark the telephone transmission with one (or both) of these identifiers of the handset. These identifiers were permanently stored in the handset long before its use in the service area of the local base station. No use of "information received by the radio receiver circuitry" would be required.

Thus, if an artisan sought to employ Hopper's teachings so that the source of annoying or threatening telephone calls could be identified, there is no reason that "*information received by the radio receiver circuitry*" would be employed.

Independent claim 55 is similarly non-obvious over the art.

Dependent claim 58 refers to combining an "overlay signal" with the data captured by the data capture system. Applicant did not intend this phrase to have so broad an interpretation as to encompass sidebands resulting from analog modulation, as taught in Hopper. Claim 58 has been amended to make clear that the combination is an *addition* operation (vs. *multiplication* – the signal processing basis for modulation); and that the overlay signal is a digital signal. Hopper does not teach such an arrangement.

Similar amendments have been made to dependent claim 60.

The rejection of independent claim 62 is also traversed.

As with claim 52, the rejection is initially flawed by its immediate identification of Hopper as a combinable reference – without consideration as to the analysis an artisan would actually undertake. That both Hopper and Reeds are in the telecommunications field should not, *per se*, relieve the Office of explaining what would have motivated an artisan, starting from Reeds, to look to Hopper.

A second ground of traverse is that the Hopper art does not teach that for which it is cited.

Claim 62 requires that the steganographic encoder is "adapted to generate an encoding signal that depends – in part – *on dynamics* of the data." Hopper does not teach this.

The Office relies on the fact that Hopper adjusts the amplitude of the data signal so that it does not cause a noticeable distortion in the speech signal (col. 5, lines 3-17). More particularly, Hopper's modulation gain is controlled by a detector (13) that tracks the magnitude of the speech, and controls the gain of the modulation signal (14) accordingly.

This arrangement is not based on dynamics, as recited in claim 62. Instead, it is based on instantaneous scaling. These are different, as explained in applicant's specification at page 10, lines 1-6:

> More satisfactory than basing the instantaneous scaling factor on a single voice data sample, is to base the scaling factor on the dynamics of several samples. That is, a stream of digitized voice data which is changing rapidly can camouflage relatively more auxiliary data than a stream of digitized voice data which is changing slowly. Accordingly, the gain control circuit 50 can be made responsive to the first, or preferably the second- or higher-order derivative of the voice data in setting the scaling factor.

Hopper's disclosure does not contain any teaching of basing a scaling factor on the dynamics of several samples. Hopper's disclosure does not contain any teaching of controlling his variable gain network 14 to be responsive to the first-, second-, or higher-order derivative of the voice information. He does not teach an encoding signal that depends on *dynamics* of the speech information. Thus, even if Hopper's teachings were employed, the arrangement of claim 62 could not result.

(New claims 73 and 74 depend from independent claim 62, and introduce limitations from the just-quoted paragraph.)

Independent claim 65 details a cell phone in which a steganographic encoder is adapted to introduce a pseudo-random signal to the data in which the hidden plural-bit auxiliary code is encoded.

Admittedly, encryption yields pseudo-random signals. However, Hopper does not teach encryption. And Reeds (which *does* employ encryption) does not teach a steganographic encoder.

If Hopper were combined with Reeds (despite the earlier-noted problems with such a starting assumption), there are two ways it might be done. Reeds' speech information could be steganographically encoded before, or after, encryption.

In the former case, steganographic encoding is applied to Reeds' plaintext speech data, and the result is then encrypted.

In the latter case, Reeds' plaintext speech data is first encrypted, and steganographic encoding is then applied to the result.

Claim 65, however, requires that it is the "steganographic encoder" that introduces the pseudo-random signal. In both of the two cases noted above, the pseudo-randomness is introduced not by the steganographic encoding; it is introduced by the encryption.

(Moreover, there is no teaching in Hopper or Reeds that would suggest encrypting the steganographic encoding. Hopper's reason for steganographically encoding the voice transmission is to permit identification of the calling party, e.g., to identify the source of annoying or threatening telephone calls. There is no incentive to prevent access to such identifying information, by encrypting same.)

Thus, even if Hopper and Reeds were combined, the arrangement of claim 65 would not result.

Independent claim 66 is rejected over Reeds in view of Hopper, and further in view of Lee (5,687,191) and Jones (3,586,781).

The Action cites Lee's normalization process (col. 7, lines 34-44) as meeting the claim 66 requirement "the steganographic encoder being adapted to increase certain of the sample value and decrease others."

It appears Lee has been misread. Col. 7, lines 34-44 describe a *prior art* psychoacoustic subband encoder. Such encoders are used in MPEG audio compression systems (i.e., MP3 compressors) to represent audio in more compact fashion. That prior art arrangement does not include any steganographic feature ("hidden data transport" to use Lee's terminology).

In ensuing disclosure, Lee details steganographic arrangements. But, contrary to the rejection, the cited normalization is not performed by Lee's steganographic encoder.

While the foregoing discussion has focused on the independent claims, the dependent claims introduce additional limitations that also contribute to their non-obviousness.

Related Application: 09/924,281

The Examiner's attention is drawn to application 09/924,281, in which the following claims are pending:

1. In a cellular telephone including a microphone, a modulator, an antenna, and an RF amplifier, the device serving to receive audio and transmit an RF signal conveying audio modulation, an improvement comprising a steganographic encoder for hiding plural bits of auxiliary data within the audio modulation of said RF signal.

2. The device of claim 1 in which said plural bits comprise data used to discourage piracy of cellular telephony service.

3. The device of claim 1 in which said plural bits comprise data identifying the cellular telephone.

4. A method of operating a cellular telephone, said telephone including a microphone coupled to a transmitter, and a receiver coupled to a transducer, the telephone serving to transmit a wireless signal modulated with a voice signal using an antenna, the method characterized by altering the voice signal to steganographically embed a multi-symbol auxiliary data string therein, wherein transmission of the wireless voice signal also conveys the auxiliary data string hidden therein.

5. In a battery-powered wireless reception device sized for fitting in a user's pocket or purse, the device including an RF amplifier, an antenna, a demodulator, and a speaker, the device serving to receive RF transmissions and output an audio signal conveyed thereby, an improvement comprising a steganographic decoder for discerning multi-symbol auxiliary data conveyed as slight alterations to said audio signal.

6. The device of claim 5 that further includes a processor to which data output by the steganographic decoder is provided.

7. In a method of operating a battery-powered wireless reception device sized for fitting in a user's pocket or purse, the device including an RF amplifier, a demodulator, an antenna, and a speaker, the device serving to receive RF transmissions and output an audio signal conveyed thereby, an improvement comprising steganographically decoding multi-symbol auxiliary data from said audio signal, and controlling some aspect of the device in accordance therewith.

8. A method comprising:

providing a digital information that is to be wirelessly transmitted to a portable device, and at said portable device be rendered in human-perceptible form to a consumer;

steganographically encoding said digital information with plural-bit auxiliary data, prior to being wirelessly transmitted;

at said portable device, recovering said auxiliary data that was steganographically encoded in said digital information;

storing said auxiliary data in said portable device; and

using said stored auxiliary data to control an aspect of the portable device's operation.

9. The method of claim 8 that includes using said stored auxiliary data to reprogram parameters of said portable device.

10. The method of claim 8 that includes transmitting digital information to plural portable devices, wherein each set of said transmitted digital information is steganographically encoded with the same plural-bit auxiliary data.

11. A method comprising:

providing a digital information that is to be wirelessly transmitted to a portable device, and at said portable device be rendered in human-perceptible form to a consumer;

steganographically encoding said digital information with plural-bit auxiliary data, prior to being wirelessly transmitted;

at said portable device, recovering said auxiliary data that was steganographically encoded in said digital information; and

using said auxiliary data to control an aspect of the portable device's operation.

12. The method of claim 11 that includes using said auxiliary data to reprogram parameters of said portable device.

13. The method of claim 11 that includes transmitting digital information to plural portable devices, wherein each set of said transmitted digital information is steganographically encoded with the same plural-bit auxiliary data.

The Examiner in 09/924,281 (Phirin Sam, Art Unit 2616) has allowed claims 8-13, and rejected claims 1-7 over Jensen (5,764,763) in view of Cooperman (5,613,004).

Cooperman is already of record in the present application; an IDS listing Jensen is submitted herewith. (Other art cited in 09/924,281, together with recently noted art, is also listed.)

The substantive contents of the most recent Action in 09/924,281 are reproduced below. Additional documents from that application are available on the online PALM/PAIR file wrapper. Or, if the present Examiner wishes, applicant can submit

copies of other documents from the file. A listing of documents in the 09/479,304 wrapper, copied from PAIR, is also presented below.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> **(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.**

2. Claims 1-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,764,763 (hereinafter referred as "Jensen") in view of US Patent 5,613,004 (hereinafter referred as "Cooperman").

Regarding claims 1-3, Jensen discloses in a cellular telephone including a microphone, a modulator, an antenna, and an RF amplifier, the device serving to receive audio and transmit an RF signal conveying audio modulation (see Figs. 1-3, 16, 17, col. 31, lines 59-67, col. 32, lines 1-5, and col. 33, col. 13-29);

Jensen does not disclose a steganographic encoder for hiding plural bits of auxiliary data within the audio modulation of said RF signal. However, Cooperman discloses a steganographic encoder for hiding plural bits of auxiliary data within the audio modulation of said RF signal (see abstract, col. 1, lines 48-57, col. 4, lines 8-27). At the time of the invention, it would have been obvious to a person of ordinary skill in the art to combine the steganographic encoder teaching by Cooperman with Jensen. The motivation for doing so would have been to provide a disincentive to piracy of material read on abstract. Therefore, it would have been obvious to combine Cooperman and Jensen to obtain the invention as specified in the claims 1-3.

EXHIBIT B

Regarding claims 4-7, Jensen discloses a method of operating a cellular telephone, said telephone including a microphone coupled to a transmitter, and a receiver coupled to a transducer, the telephone serving to transmit a wireless signal modulated with a voice signal using an antenna (see Figs. 1-3, 16, 17, col. 31, lines 59-67, col. 32, lines 1-5, and col. 33, col. 13-29);

Jensen does not disclose altering the voice signal to steganographically embed a multi-symbol auxiliary data string therein, wherein transmission of the wireless voice signal also conveys the auxiliary data string hidden therein. However, Cooperman discloses steganographically embed a multi-symbol auxiliary data string and conveys the auxiliary data string hidden (see abstract, col. 1, lines 48-57, col. 4, lines 8-27). At the time of the invention, it would have been obvious to a person of ordinary skill in the art to combine steganographically embed a multi-symbol auxiliary data string and conveys the auxiliary data string hidden teaching by Cooperman with Jensen. The motivation for doing so would have been to provide a disincentive to piracy of material read on abstract. Therefore, it would have been obvious to combine Cooperman and Jensen to obtain the invention as specified in the claims 4-7.

Allowable Subject Matter

3. Claims 8-13 are allowed.

Response to Arguments

4. Applicant's arguments with respect to claims 1-7 have been considered but are moot in view of the new ground(s) of rejection.

09/924,261 WIRELESS METHODS AND DEVICES EMPLOYING STEGANOGRAPHY

Transaction History

Transaction History

Date	Transaction Description
10-04-2007	Case Docketed to Examiner in GAU
08-21-2007	Mail Non-Final Rejection
08-18-2007	Non-Final Rejection
06-07-2007	Information Disclosure Statement considered
06-07-2007	Reference capture on IDS
06-07-2007	Information Disclosure Statement (IDS) Filed
06-11-2007	Date Forwarded to Examiner
06-07-2007	Response after Non-Final Action
06-07-2007	Information Disclosure Statement (IDS) Filed
04-18-2007	Mail Non-Final Rejection
04-13-2007	Non-Final Rejection
02-15-2007	Information Disclosure Statement considered
02-15-2007	Reference capture on IDS
02-15-2007	Information Disclosure Statement (IDS) Filed
02-15-2007	Information Disclosure Statement (IDS) Filed
02-03-2007	Date Forwarded to Examiner
01-22-2007	Response after Non-Final Action
12-12-2006	Mail Non-Final Rejection
12-11-2006	Non-Final Rejection
10-03-2006	Date Forwarded to Examiner
10-02-2006	Response after Non-Final Action
10-02-2006	Request for Extension of Time - Granted
06-14-2006	Mail Non-Final Rejection
06-12-2006	Non-Final Rejection
04-07-2006	Date Forwarded to Examiner
04-07-2006	Withdrawal of Notice of Allowance
03-22-2006	Mail Notice of Allowance
03-22-2006	Mail Notification of Terminal Disclaimer - Accepted
03-21-2006	Case Docketed to Examiner in GAU
03-20-2006	Notice of Allowance Data Verification Completed
03-20-2006	Case Docketed to Examiner in GAU
03-20-2006	Paralegal TD Accepted
03-20-2006	Notification of Terminal Disclaimer - Accepted
08-07-2001	Terminal Disclaimer Filed
03-16-2006	terminal disclaimer fee paid
03-10-2006	Date Forwarded to Examiner
03-02-2006	Response after Non-Final Action
03-02-2006	Request for Extension of Time - Granted
10-27-2005	Mail Non-Final Rejection
10-26-2005	Non-Final Rejection
07-01-2005	Reference capture on IDS

07-01-2005	Information Disclosure Statement (IDS) Filed
07-01-2005	Information Disclosure Statement (IDS) Filed
07-08-2005	Date Forwarded to Examiner
07-01-2005	Response after Non-Final Action
03-30-2005	Mail Non-Final Rejection
03-28-2005	Non-Final Rejection
03-15-2005	Case Docketed to Examiner in GAU
01-26-2005	Case Docketed to Examiner in GAU
09-22-2004	Case Docketed to Examiner in GAU
07-19-2004	IFW TSS Processing by Tech Center Complete
08-07-2001	Reference capture on IDS
05-19-2004	Miscellaneous Incoming Letter
03-11-2002	Case Docketed to Examiner in GAU
08-07-2001	Information Disclosure Statement (IDS) Filed
08-07-2001	Information Disclosure Statement (IDS) Filed
11-20-2001	Case Docketed to Examiner in GAU
11-03-2001	Application Dispatched from OIPE
11-02-2001	Application Is Now Complete
08-30-2001	Notice Mailed--Application Incomplete--Filing Date Assigned
08-27-2001	Correspondence Address Change
08-21-2001	IFW Scan & PACR Auto Security Review
08-07-2001	Initial Exam Team nn

Applicant called the present application to the attention of Examiner Sam in applicant's last communication in that case, in June 2007.

In the IDS submitted herewith are commonly-owned patents and applications, 6,064,737, 6,278,781 and 20070189533, to which the Examiner's attention is particularly directed in connection with possible double-patenting issues.

The Examiner is invited to telephone the undersigned if it might help bring prosecution of this application to a close.

Respectfully submitted,

Date: October 11, 2007

DIGIMARC CORPORATION

CUSTOMER NUMBER 23735

By _____

Phone: 503-469-4800
FAX 503-469-4777

William Y. Conwell
Registration No. 31,943

Department of Public Safety & Oregon State Police

Operation ID

Crime Prevention

General Prevention | Operation ID Program | Property Crimes
What is Suspicious? | Crimes Against a Person

The Operation ID program encourages documentation and engraving of personal property, equipment, and bicycles on campus. The program will help to deter theft and aid in returning recovered property. On this form you will list descriptions of valuable items, serial numbers and any owner engraved identification. If any item is stolen and you have the serial number, the item can be entered in a national Law Enforcement computer system and can be identified anywhere in the US.

If you need to use an engraver to mark a number on your items, they are available at all residence halls, co-ops, and at the Department of Public Safety Office. They may be checked out at no cost to students, faculty, and staff. Questions: please call 737-3010.

Please print this page, fill it out, and retain it for possible future use.

ITEM	BRAND	DESCRIPTION	SERIAL NUMBER	$ VALUE
Bicycle				
Stereo Equipment				
Computer Equipment				
VCR/DVD				
Television				
Watches and Jewelry				
Calculators				

EXHIBIT A

EXHIBIT B

Car Stereo Equipment				
Misc.				

Never Take Chances With Your Health & Safety!
Campus Emergency Dial 737-7000
Off-Campus Emergency Dial 911
Non-Emergency 737-3010
200 Cascade Hall

The Department of Public Safety & Oregon State Police,
200 Cascade Hall, Oregon State University Corvallis, OR 97331. 541-737-3010
Contact us with your comments, questions and feedback
Copyright © 2007 Oregon State University | **Disclaimer**

EXHIBIT A

EXHIBIT B

January 22, 2004

U.S. Department of Justice
Federal Bureau of Investigation
11000 Wilshire Blvd.
Los Angeles, CA 90024
(310) 996-3345, 3342, 3343, 3804
Fax: (310) 996-3345

Chicago Man Arrested For Criminal Copyright Infringement in Connection

with Prohibited Release of Major Motion Pictures, Many Prior to their Theatrical Release

Acting Assistant Director in Charge of the FBI's Los Angeles Field Office James Sheehan announced today the arrest of William Sprague, a resident of Homewood, Illinois (a suburb of Chicago) on charges of criminal copyright infringement and illegal interception of a satellite signal. The arrest was made in connection with a Los Angeles-based investigation into the compromise of a multitude of major motion pictures that surfaced on the Internet, many prior to their theatrical and/or DVD release. Among the movies released by an Internet pirating group are Master and Commander, Last Samurai, Matrix Revolutions, Mystic River, Gods and Generals, Mighty Wind, Matchstick Men, Something's Gotta Give, Love Actually, Thirteen, Calendar Girls. The major film studios affected by these releases are Warner Brothers, Sony Pictures, Universal, Fox, and Disney. Forensic analysis of the film content posted on the Internet revealed that many of the compromised movies were derived from Academy screeners that were embedded with a new digital watermark that discretely identifies the individual screening tape. This watermark can then be linked to the recipient of the screener.

Most of the compromised movies listed above had been provided to Carmine Caridi, a veteran actor of film and television, and a member of the Academy of Motion Picture Arts and Sciences for approximately 22 years. Investigation of Caridi revealed that for at least the last three years, he had supplied Russell William Sprague with virtually every Academy screener (approximately 60 movies per year). A search warrant at the Sprague residence in Illinois was executed with the assistance of the FBI's Chicago Division today. Hundreds of Academy screeners were seized, many of which had been converted to DVD, along with an array of duplication equipment. A quantity of illegal satellite television interception equipment was also seized during the search.

Sprague will be afforded an initial appearance in U.S. District Court in Chicago tomorrow.

The public is reminded that a criminal complaint contains only allegations of misconduct and that the defendant is presumed innocent until and unless proven guilty in a court of law.

###

EXHIBIT B

EXHIBIT B

April 13, 2004

U.S. Department of Justice
Assistant United States Attorney
Christopher Johnson
Central District of California
(213) 894-2688

Illinois Man who Distributed Illegally Copied Movies Pleads Guilty to Federal Copyright Infringement Charges

An Illinois man has pleaded guilty to federal copyright infringement charges for reproducing and distributing more than 200 Academy Award "screeners."

Russell William Sprague, 51, of Homewood, Illinois, pleaded guilty yesterday to one felony count of criminal copyright infringement. Sprague obtained the movies - which included "Master and Commander: The Far Side of the World" and "House of Sand and Fog" - from an actor who was a member of the Academy of Motion Picture Arts and Sciences. The actor - Carmine Caridi, who has since been expelled from the Academy - received copies of dozens of Oscar-nominated films every year. Sprague took the screeners in VHS tape format, digitized the films and produced illegal DVDs that were distributed to a variety of persons.

The case against Sprague resulted from an investigation into Internet postings of seven feature films that had been nominated for Academy Awards. Forensic analysis of the films posted on the Internet revealed that many of the movies were derived from Academy screeners that had been embedded with a new digital watermark that discretely identifies individual screening tapes. This watermark on all seven movies linked them to actor Carmine Caridi, who admitted sending copies of his screeners to Sprague in Illinois.

Sprague was arrested pursuant to a criminal complaint on January 22. He was freed on bond, and he was indicted by a federal grand jury in Los Angeles on February 12. Sprague pleaded guilty before United States District Judge George H. King, who is scheduled to sentence him on July 26. At sentencing, Sprague faces a maximum penalty of three years in federal prison.

The case against Sprague is the result of an investigation conducted by the Federal Bureau of Investigation.

Release No. 04-049

###

EXHIBIT C

EXHIBIT B

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/670,841	02/02/2007	Geoffrey B. Rhoads	P1271	7876

23735 7590 09/14/2007

DIGIMARC CORPORATION
9405 SW GEMINI DRIVE
BEAVERTON, OR 97008

EXAMINER	
SAM, PHIRIN	

ART UNIT	PAPER NUMBER
2616	

MAIL DATE	DELIVERY MODE
09/14/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Docketed: 12-14-07

Book: _____ Init: _____

RECEIVED
SEP 17 2007
DIGIMARC

EXHIBIT C

Office Action Summary	Application No.	Applicant(s)	
	11/670,841	RHOADS, GEOFFREY B.	
	Examiner	Art Unit	
	Phirin Sam	2616	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 February 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12 and 21-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *12* is/are allowed.

6)☒ Claim(s) *1-11 and 21-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02 February 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

PHIRIN SAM
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-11 and 21-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,392,356 (hereinafter referred as "Konno") in view of US Patent 5,613,004 (hereinafter referred as "Cooperman").

Regarding claims 1, 2, and 8-11, Konno discloses a method of operating a wireless telephone device (see Figs. 1 and 2, col. 5, lines 21-27), characterized by decoding plural-bit data in digital information processed by said wireless telephone device (see Figs. 1 and 2, col. 5, lines 46-58), and controlling an aspect of the device's operation based on said decoded data (see Figs. 1 and 2, col. 5, lines 28-36, col. 6, lines 58-68).

Konno does not disclose steganographically encoded. However, Cooperman discloses steganographically encoded (see col. 7, lines 9-35, 61-64). At the time of the invention, it would have been obvious to a person of ordinary skill in the art to combine steganographically encoded data teaching by Cooperman with Konno. The motivation for doing so would have been to provide to carry the hidden message does not know it contains this hidden message and therefore it does not obtain the information in the hidden message read on column 1, lines 53-55. Therefore, it would have been obvious to combine Cooperman and Konno to obtain the invention as specified in the claims 1, 2, and 8-10.

Regarding claims 3-7, Konno does not disclose filtering the digital information, removing operation, matching filtering, correlation, and alignment. However, Cooperman discloses filtering the digital information, removing operation, matching filtering, correlation, and alignment (see col. 9, lines 46-62, col. 12, lines 33-67, and col. 13, lines 1-13). At the time of the invention, it would have been obvious to a person of ordinary skill in the art to combine filtering the digital information, removing operation, matching filtering, correlation, and alignment teaching by Cooperman with Konno. The motivation for doing so would have been to provide to carry the hidden message does not know it contains this hidden message and therefore it does not obtain the information in the hidden message read on column 1, lines 53-55. Therefore, it would have been obvious to combine Cooperman and Konno to obtain the invention as specified in the claims 3-7.

Regarding claims 21-23, Konno discloses a wireless telephone device (see Figs. 1 and 2, col. 5, lines 21-27) characterized by a decoder operative to recover data from digital information processed by said device (see Figs. 1 and 2, col. 5, lines 46-58), and further including a processor operative to control an aspect of the wireless telephone device's operation based on the recovered data (see Figs. 1 and 2, col. 5, lines 28-36, and col. 6, lines 58-68).

Konno does not disclose steganographically-encoded data. However, Cooperman discloses steganographically-encoded data (see col. 7, lines 9-35, 61-64). At the time of the invention, it would have been obvious to a person of ordinary skill in the art to combine steganographically encoded data teaching by Cooperman with Konno. The motivation for doing so would have been to provide to carry the hidden message does not know it contains this hidden message and therefore it does not obtain the information in the hidden message read on column

1, lines 53-55. Therefore, it would have been obvious to combine Cooperman and Konno to obtain the invention as specified in the claims 21-23.

Allowable Subject Matter

3. Claim 12 is allowed.

Conclusion

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Phirin Sam whose telephone number is (571) 272-3082. The examiner can normally be reached on a compress schedule, from 8:00-5:30, first Wed off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jay Patel can be reached on (571) 272 - 2988. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Respectfully submitted,

Date: September 11, 2007

PHIRIN SAM
PRIMARY EXAMINER

EXHIBIT C

Notice of References Cited	Application/Control No. 11/670,841	Applicant(s)/Patent Under Reexamination RHOADS, GEOFFREY B.	
	Examiner Phirin Sam	Art Unit 2616	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-5,613,004	03-1997	Cooperman et al.	380/28
*	B	US-5,392,356	02-1995	Konno et al.	380/249
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

EXHIBIT C